REMARKS

Applicant wishes to thank the Examiner for reviewing the present application. Applicant also wishes to thank the Examiner for taking the time to meet with the undersigned in the Personal Interview conducted on January 24, 2006.

In the above Interview, claims 1-3 were discussed. The Examiner indicated that claim 1 would be allowable over the Vanstone reference if claim 1 were amended to reflect that the method is applied to an MQV protocol as mentioned in steps a-d. The rejection of claim 2 regarding the expressions "third exponent" and "fourth exponent" was also discussed in the interview. It was agreed that the above expressions should read "one exponent" and "other exponent" respectively. Applicant refers to the Interview Summary, a copy of which is attached with this response.

Amendments to the Claims

Claim 1 is amended reflecting that the method is applied to an MQV key generation protocol as agreed upon in the above mentioned Interview.

Claim 2 is amended replacing "third" with "one" and "fourth" with "other".

No new subject matter is believed to have been added by way of these amendments.

Claim Rejections – 35 U.S.C. §112

Claims 2-3 have been rejected under 35 U.S.C. §112, first paragraph as failing to comply with the enablement requirement. As noted above, claim 2 is amended to overcome this rejection as discussed in the Interview of January 24, 2006. Therefore, claims 2-3 are submitted to comply with 35 U.S.C. §112, first paragraph.

Claim Rejections – 35 U.S.C. §103

Claims 1-8 have been rejected under 35 U.S.C. §103(a) as being unpatentable over US Patent No. 5,889,865 to Vanstone et al. in view of US Patent No. 5,987,131 to Clapp. As noted above, claim 1 is amended as agreed upon in the above mentioned Interview, and as such, amended claim 1 is believed to comply with 35 U.S.C. §103(a).

Claim 1 relates to the use of simultaneous exponentiation with the MQV protocol,

recognizing that the same can be done by rearranging certain terms in the MQV protocol for efficient computation using a simultaneous exponentiation technique. As discussed in the above mentioned Interview, and noted above, amended claim 1 is believed to distinguish over the Vanstone reference.

Clapp teaches a method for cryptographic key exchange using modular exponentiation and storing pre-computed values. Applicant respectfully submits that Clapp does not teach simultaneous exponentiation as required by claim 1 (and missing from Vanstone), let alone teach the rearrangement of terms recited in the claims. Clapp therefore fails to teach what is missing from Vanstone.

Accordingly, Applicant believes that amended claim 1 clearly and patentably distinguishes over the prior art cited by the Examiner and as such is in condition for allowance.

Claims 2-8 being ultimately dependent on claim 1 are also believed to overcome the prior art.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: Feb 25, 2006

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL